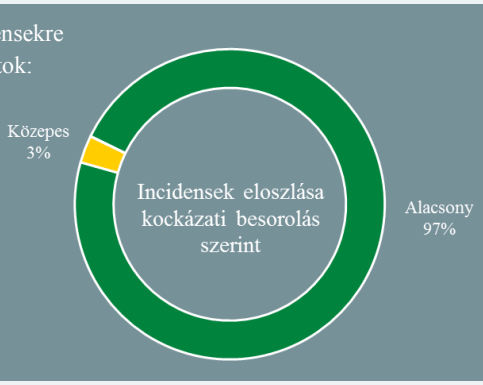
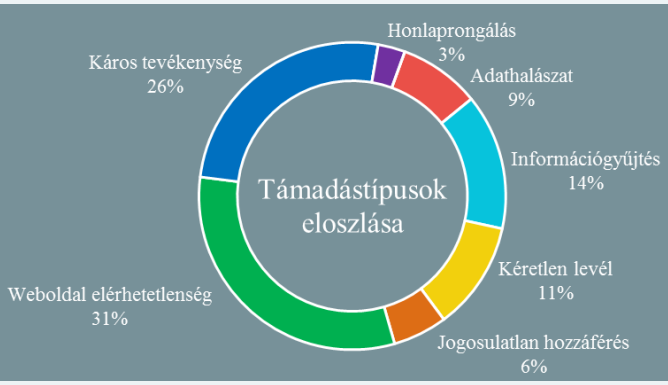
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 33. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.08.07. - 2020.08.13.





Kövessen minket megújult weboldalunkon, ahol friss IT-biztonsági hírek kerülnek publikálásra!

TeamViewer felhasználók figyelem: frissítsenek a legutóbbi verzióra!

(thehackernews.com)

TeamViewer felhasználók számára erősen javasolt a CVE 2020-13699 számú sérülékenységet javító biztonsági frissítés telepítése, ugyanis a hiba lehetővé teheti, hogy egy támadó egy viszonylag könnyen kivitelezhető támadás során ellopja jelszavukat. A TeamViewer egy népszerű távmenedzsment eszköz, ami több platformra ─ például Windows, macOS, Linux, Chrome OS, iOS, Android, Windows RT, Windows Phone 8, és BlackBerry ─ is elérhető. A sérülékenység lehetővé teheti, hogy a támadó egy speciálisan szerkesztett honlap segítségével arra kényszerítse a TeamViewer klienst, hogy az egy autentikációs folyamatot indítson a támadó irányítása alatt álló fájlmegosztás felé, amelynek során a felhasználói fiók neve és a hozzá tartozó jelszó hash is elküldésre kerül, rossz kezekbe. **Bővebben...**

DEF CON: komoly biztonsági hiba érintette a Samsung telefonok 'Find My Mobile" funkcióját

(securityweek.com)

Négy, egymás után kihasználható sérülékenységere hívta fel a figyelmet a pénteki DEF CON konferencián Pedro Umbelino, a portugál székhelyű Char49 kiberbiztonsági cég egy kutatója. A sebezhetőségek kihasználásával egy rosszindulatú alkalmazás képes lehetett volna ugyanarra, mint a Find My Mobile funkció, azaz például a gyári beállítások visszaállítására, adatok törlésére, az eszköz helyzetének valós időben történő nyomkövetésére, telefonhívások és üzenetek lekérdezésére, valamint a készülék zárolására, vagy feloldására. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat arról, hogy mik lehetnek a jelei egy folyamatban lévő zsarolóvírus támadásnak.

A nagy kínai tűzfal update: TLS 1.3-as kapcsolatok blokkolva

(zdnet.com)

Kína fejlesztéseket végzett legismertebb cenzúra eszközén, a Nagy Tűzfalon (GFW), annak érdekében, hogy a webes forgalom megfigyelését megakadályozó TLS 1.3 és az ESNI (Encrypted Server Name Indication) protokollokat használó titkosított HTTPS kapcsolatok blokkolásra kerüljenek. Más, korábbi protokollokat alkalmazó (TLS 1.1, TLS 1.2, SNI) kapcsolatokra nem vonatkozik a tiltás, ezek esetében ugyanis a kínai kormányzat meg tudja állapítani, hogy melyik weboldal került meglátogatásra.

Ügyes adathalász üzenettel próbálták megszerezni cPanelt használók bejelentkezési adatait

(bleepingcomputer.com)

cPanel és WebHost Manager (WHM) felhasználókat céloz egy új, cseles adathalász kampány. A rendkívül megtévesztő "cPanel Urgent Update Request" tárgyú üzenet első ránézésre több szempontból is hitelesnek tűnhet: egy kritikus sebezhetőség miatt kiadott javításról szól, nem tartalmaz helyesírási hibákat, az Amazon Simple Email Service (SES) szolgáltatón keresztül került kiküldésre, sőt a támadók a cpanel7831.com domaint is beregisztrálták a hitelesség kedvéért. **Bővebben...**

Egy nehezen javítható tervezési hiba miatt a Microsoft Teams frissítéskezelője kihasználható káros kódok telepítésére

(securityaffairs.co)

A Trustwave biztonsági szakemberei egy veszélyes, „Living-Off-the-Land" típusú technikával kihasználható biztonsági hibát azonosítottak a Microsoft Teams frissítéskezelőjében (MS Teams Updater), ami egy támadó számára lehetővé teheti tetszőleges kód letöltését és futtatását az áldozat rendszerén. A hiba abból fakad, hogy bár egy korábbi patch az URL-en keresztüli frissítést megszüntette a Teams Updaterben, az UNC (Universal Naming Convention) formátumban megadott eléréseket nem. **Bővebben...**